CLAIMS

1. A system for secure communication across a communication network characterised by comprising:

a personal code generation means having one or more identification codes and one or more encryption codes, the or each identification code and the or each encryption code being arranged to change at predetermined time intervals; and

a code server synchronised with the personal code generation means such that the code server has information regarding the or each current identification code and the or each current encryption code of the personal code generation means;

wherein a user transmits across the communication network, the or each current identification code of the personal code generation means and data encrypted with the or each current encryption code of the personal code generation means and the code server uses the information regarding the or each current identification code to authenticate the user and the information about the or each current encryption code to decrypt the transmitted data.

2. A system for secure communication in accordance with claim 1 characterised in that the code server communicates to the user following authentication of the user by transmitting data across the communication network to the user encrypted with the or each current encryption code and the user decrypts the data transmitted by the code server with the or each corresponding current encryption code of the personal code generation means.

3. A system for secure communication in accordance with claim 1 or claim 2, characterised in that the code server stores information including a username assigned

to the owner of the personal code generation means and the username is transmitted across the communication network with the or each current identification code and the data encrypted with the or each current encryption code and the code server uses the username to authenticate the user as the owner of the personal code generation means.

4. A system for secure communication in accordance with any one of claims 1 to 3, characterised in that the code server stores information including a password assigned to the owner of the personal code generation means and the password is transmitted across the communication network with the or each current identification code and the data encrypted with the or each current encryption code and the code server uses the password to authenticate the user as the owner of the personal code generation means.

5. A system for secure communication in accordance with any one of claims 1 to 4, characterised in that the personal code generation means comprises a personal portable token.

6. A system for secure communication in accordance with claim 5, wherein the personal portable token is a pendant.

7. A system for secure communication in accordance with claim 5, wherein the personal portable token is a card.

8. A system for secure communication in accordance with any one of claims 5 to 7, characterised in that the personal code generation means includes a communication port to communicate the or each current identification code and the or each current encryption code to a user's computer.

9. A system for secure communication in accordance with any one of claims 1 to 4, characterised in that the personal code generation means comprises software residing on a user's computer.

10. A system for secure communication in accordance with claim any one of claims 5 to 9, characterised in that the personal code generation means includes a display means, the display means displaying the or each current identification code and the or each current encryption code.

11. A system for secure communication in accordance with claim 5, characterised in that the personal code generation means comprises a smart card having an initialisation code known to the code server and software residing on a user's computer, the software being capable of generating the or each current identification code and the or each current encryption code based on the initialisation code and a reference clock, the code server also being capable of generating the or each current identification code and the or each current encryption code based on the initialisation code and the reference clock.

12. A system for securely accessing data stored in an encrypted form on a storage means accessible by a communication network comprising:

a personal code generation means having one or more identification codes and one or more encryption codes, the or each identification and the or each encryption code being arranged to change at predetermined time intervals;

a key archive associated with the personal code generation means and with one or more data files on the storage means, the key archive having information including the location of the data files and the encryption codes with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and

a code server synchronised with the personal code generation means such that the code server has information regarding the or each current identification code and the or each current encryption code of the personal code generation means, the code server also having a previous archiving code being the archiving code last used to encrypt the key archive and a current archiving code being arranged to change at predetermined time intervals;

wherein when a user wishes to access the or each stored data file, the user transmits across the communication network, the or each current identification code and data including a request to access the stored data files and the code server uses the information regarding the or each current identification code to authenticate the user and the information about the or each current encryption code to decrypt the transmitted data and the code server communicates to the user the previous archiving code in encrypted form using the or each current encryption code so that the user may decrypt the key archive providing access to the stored data files.

13. A system for securely accessing data stored in accordance with claim 12, wherein when the code server transmits to the user the previous archiving code, the code server also transmits the current archiving code and the user then uses the current archiving code to encrypt the key archive when the user has completed accessing the stored data files and the code server stores the current archiving code as the previous archiving code for future access to the store data files.

14. A method for securely communicating across a communication network characterised by comprising the steps of:

providing a personal code generation means to a user, the personal code generation means having one or more identification codes and one or more encryption codes, the

or each identification code and the or each encryption code being arranged to change at predetermined time intervals; and

providing a code server and synchronising the code server with the personal code generation means such that the code server has information regarding the or each current identification code and the or each current encryption code of the personal code generation means; and

the user transmitting across the communication network, the or each current identification code of the personal code generation means and data encrypted with the or each current encryption code of the personal code generation means and the code server using the information regarding the or each current identification code to authenticate the user and the information about the or each current encryption code to decrypt the transmitted data.

15. A method for securely communicating across a communication network in accordance with claim 14 including the step of the code server communicating to the user following authentication of the user by transmitting data across the communication network to the user encrypted with the current encryption code and the user decrypting the data transmitted by the code server with the corresponding current encryption code of the personal code generation means.

16. A method for securely communicating across a communication network in accordance with claim 14 or claim 15, including the steps of providing the user with a username and password known to the code server and transmitting the username and password across the communication network with the or each current identification code and the data encrypted with the or each current encryption code and the code

server using the username and password to authenticate the user of the personal code generation means.

17. A method for securely accessing data stored in an encrypted form on a storage means accessible by a communication network comprising the steps of:

providing a personal code generation means having one or more identification codes and one or more encryption codes, the or each identification and the or each encryption code being arranged to change at predetermined time intervals;

providing a key archive associated with the personal code generation means and with one or more data files on the storage means, the key archive having information including the location of the data files and encryption keys with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and

synchronising the personal code generation mean with a code server such that the code server has information regarding the or each current identification code and the or each current encryption code of the personal code generation means, the code server also having a previous archiving code being the archiving code last used to encrypt the key archive and a current archiving code being arranged to change at predetermined time intervals;

the user transmitting across the communication network, the or each current identification code and data including a request to access the stored data files encrypted with the or each current encryption code;

the code server using the information regarding the or each current identification code to authenticate the user and the information about the or each current encryption code to decrypt the transmitted data and the code server communicating to the user the

previous archiving code in encrypted form so that the user may decrypt the key archive providing access to the stored data files.

18. A method for securely accessing data stored in an encrypted form on a storage means accessible by a communication network in accordance with claim 17 including the steps of:

the user using the current archiving code to encrypt the key archive on completing accessing the stored data files; and

the code server storing the current archiving code as the previous archiving code for future access to the store data files.